The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/25/2009

SUBJECT:
Vulnerability in IBM Lotus Notes client could lead to Remote Code Execution

OVERVIEW:

Lotus Notes is a collaborative software used for accessing e-mail, calendars and other applications. A new vulnerability has been discovered in the client side of this software which can be exploited if a user opens an email and views a malicious Microsoft Excel attachment. Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user account, an attacker could then install programs; view, change, or delete data; or create new accounts. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

- IBM Lotus Notes 6.5.0
- IBM Lotus Notes 6.5.1
- IBM Lotus Notes 6.5.2
- IBM Lotus Notes 6.5.3
- IBM Lotus Notes 6.5.4
- IBM Lotus Notes 6.5.5
- IBM Lotus Notes 6.5.5 FP2
- IBM Lotus Notes 6.5.5 FP3
- IBM Lotus Notes 6.5.6
- IBM Lotus Notes 6.5.6 FP2
- IBM Lotus Notes 7.0
- IBM Lotus Notes 7.0.1
- IBM Lotus Notes 7.0.2
- IBM Lotus Notes 7.0.2 FP1
- IBM Lotus Notes 7.0.3
- IBM Lotus Notes 8.0
- IBM Lotus Notes 8.5

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:

The Lotus Notes client, which is primarily used for accessing e-mail, calendars and applications on an IBM Lotus Domino server is susceptible to a buffer overflow vulnerability. This vulnerability is in the File Attachment Viewer (xlssr.dll) of IBM Lotus Notes client, which is the default viewer for all attachments in Lotus Notes. This vulnerability exists due to inadequate boundary check on user supplied data on the affected application that can be exploited if a user opens an email and views a malicious Microsoft Excel attachment.

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user account, an attacker could then install programs; view, change, or delete data; or create new accounts. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:

The following actions should be taken:

- Remind users not to open email attachments from unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply appropriate patches provided by IBM to vulnerable systems immediately after appropriate testing.
- If patching is not possible at this time, consider the following workarounds:
    - Deleting the keyview.ini file in the Notes program directory. This disables ALL viewers.
    - Deleting or renaming the associated DLL file. The viewer associates the Microsoft Excel file with xlssr.dll.
    - Comment out the reference to the DLL file in the keyview.ini by placing a semi-colon ";" at the beginning of the line containing the associated DLL file.
    - If any of these are used when a user clicks View, for any file, a dialog box will display with the message "Unable to locate the viewer configuration file." The user would then need to download or save the attachment and open the attachment with the appropriate software.
    - Consider employing Data Execution Prevention (DEP) to limit successful attacks. More information on DEP and how to enable it can be found at http://support.microsoft.com/kb/889741.

REFERENCES:

IBM:

http://www-01.ibm.com/support/docview.wss?uid=swg21396492

Security Focus:
http://www.securityfocus.com/bid/36124

Secunia:
http://secunia.com/advisories/36472/

http://secunia.com/advisories/36474/